FIPS 201 REQUIREMENT TRACEABILITY MATRIX

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
1-1	The organization shall adopt and use an approved identity proofing and registration process.	2.2/6	PIV Identity Proofing and Registration Requirements	Identity proofing and registration	Card Issuance and Management	PIV System	Process	G	
1-2	The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. At a minimum, the National Agency Check (NAC) shall be completed before credential issuance. Appendix C, Background Check Descriptions, provides further details on NAC and NACI.	2.2/6	PIV Identity Proofing and Registration Requirements	Identity proofing and registration	Card Issuance and Management	IDMS	Process	S	
1-3	The applicant must appear in-person at least once before the issuance of a PIV credential.	2.2/6	PIV Identity Proofing and Registration Requirements	Identity proofing and registration	Card Issuance and Management	IDMS	Process	S	
1-4	During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No.	2.2/6	PIV Identity Proofing and Registration Requirements	Identity proofing and registration	Card Issuance and Management	IDMS	Process	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture identification (ID).								
1-5	The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.	2.2/6	PIV Identity Proofing and Registration Requirements	identity proofing and registration	Card Issuance and Management	PIV System	Process	G	
1-6	Assign an individual to the role of senior agency official for privacy. The senior agency official for privacy is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard. The individual serving in this role may not assume any other operational role in the PIV system.	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	S	
1-7	Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with [E-Gov] and [OMB322]. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	S	
1-8	Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, personal information in identifiable form [IIF]), the purpose of collection, what information may be disclosed to whom during	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. PIV applicants shall be provided full disclosure of the intended uses of the PIV credential and the related privacy implications								
1-9	Assure that systems that contain IIF for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY]. the Privacy Act of 1974 [PRIVACY]	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	G	
1-10	Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	S	
1-11	Ensure that only personnel with a legitimate need for access to IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	G	
1-12	Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.	2.4/7	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	G	
1-13	Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.	2.4/8	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	G	
1-14	Utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information	2.4/8	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	Systems, to accomplish privacy goals, where applicable. [SP800-53]								
1-15	Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential.	2.4/8	PIV Privacy Requirements	PIV System Privacy	Card Issuance and Management	PIV System	Process	G	
2-1	The PIV Card shall comply with physical characteristics as described in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443].	4.1/15	Physical PIV Card Topology	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-2	The printed material shall not rub off during the life of the PIV Card, nor shall the printing process deposit debris on the printer rollers during printing and laminating.	4.1.1/15	Physical PIV Card Topology	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-3	Printed material shall not interfere with the contact and contactless ICC(s) and related components, nor shall it obstruct access to machine-readable information.	4.1.1/15	Physical PIV Card Topology	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-4	The PIV Card shall contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. At a minimum, a PIV Card shall incorporate one such security feature. Examples of these security features include the following: + Optical varying structures + Optical varying inks	4.1.2/15	Tamper Proofing and Resistance	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	+ Laser etching and engraving + Holograms + Holographic images + Watermarks.								
2-5	Incorporation of security features shall— + Be in accordance with durability requirements [ISO7810] + Be free of defects, such as fading and discoloration + Not obscure printed information + Not impede access to machine-readable information.	4.1.2/16	Tamper Proofing and Resistance	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-6	The PIV Card shall contain a contact and a contactless ICC interface.	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-7	The card body structure shall consist of card material(s) that satisfy the card characteristics in [ISO7810] and test methods in American National Standards Institute (ANSI) 322. [ANSI322] Although the [ANSI322] test methods do not currently specify compliance requirements, the tests shall be used to evaluate card material durability and performance. The [ANSI322] tests minimally shall include card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet light exposure, and a laundry test. Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture. The reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a two percent soap solution.	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
2-8	The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect 2000 hours of southwestern United States' sunlight exposure in accordance with [ISO10373], Section 5.12. Concentrated sunlight exposure shall be performed in accordance with [G90-98] and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading resistance and subjected to the same [ISO10373] dynamic bending test.	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-9m	The card shall be 27- to 33-mil thick (before lamination) in accordance with [ISO7810].	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-10m	The PIV Card shall not be embossed.	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-11m	Decals shall not be adhered to the card.	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-12m	Departments and agencies may choose to punch an opening in the card body to enable the card to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity is not adversely impacted. Departments and agencies are strongly	4.1.3/16	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	encouraged to ensure such alterations do not— • Compromise card body durability requirements and characteristics • Invalidate card manufacturer warranties or other product claims • Alter or interfere with printed information, including the photo • Damage or interfere with machine-readable technology, such as the embedded antenna.								
2-13	The card material shall withstand the effects of temperatures required by the application of a polyester laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer shall not interfere with the smart card reader operation. The card material shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.	4.1.3/17	Physical Characteristics and Durability	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-14	The information on a PIV Card shall be in visual printed and electronic form.	4.1.4/17	Visual Card Topography	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-15	Printed data shall not interfere with machine-readable technology.	4.1.4/17	Visual Card Topography	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-16	Areas that are marked as reserved should not be used for printing.	4.1.4/17	Visual Card Topography	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-17	The photograph shall be placed in the upper left corner and be a full frontal pose from top of the head to shoulder, as depicted in Figure 4-1. A minimum of 300 dots per inch (dpi)	4.1.4.1/17	Mandatory Items on the Front of the PIV Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	resolution shall be used. The background should follow recommendations set forth in SP 800-76.								
2-18	The full name shall be printed directly under the photograph in capital letters. The font shall be a minimum of 10 point.	4.1.4.1/18	Mandatory Items on the Front of the PIV Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-19	A printed employee affiliation shall be printed on the card. Some examples of employee affiliation are "CONTRACTOR," "ACTIVE DUTY," and "CIVILIAN."	4.1.4.1/18	Mandatory Items on the Front of the PIV Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-20	The Organizational Affiliation shall be printed as depicted in Figure 4-1.	4.1.4.1/18	Mandatory Items on the Front of the PIV Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-21	The card expiration date shall be printed in a YYYYMMMDD format.	4.1.4.1/18	Mandatory Items on the Front of the PIV Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-22	Agency Card Serial Number- This item shall be printed as depicted in Figure 4-6 and contain the unique serial number from the issuing department or agency. The format shall be at the discretion of the issuing department or agency.	4.1.4.2/18	Mandatory Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-23	Issuer Identification- This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.	4.1.4.2/18	Mandatory Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-24	Zone 3—Signature. If used, the department or agency shall place the cardholder signature below the photograph and cardholder name as depicted in Figure 4-3. The space for the signature shall not interfere with the contact and	4.1.4.3/18	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	contactless placement. Because of card topology space constraints, placement of a signature may limit the size of the optional two-dimensional bar code.								
2-25	Zone 4—Agency Specific text area. If used, this area can be used for printing agency specific requirements, such as employee status.	4.1.4.3/18	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-26	Zone 5—Rank. If used, the cardholder's rank shall be printed in the area as illustrated. Data format is at the department or agency's discretion.	4.1.4.3/18	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-27	Zone 6—Portable Data File (PDF) Two-Dimensional Bar Code. If used, the PDF bar code placement shall be as depicted in the diagram (i.e., left side of the card). If Zone 3 (a cardholder signature) is used, the size of the PDF bar code may be affected. The card issuer should confirm that a PDF used in conjunction with a PIV Card containing a cardholder signature will satisfy the anticipated PDF data storage requirements.	4.1.4.3/18	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-28	Zone 9— Header. If used, the text "United States Government" shall be placed as depicted in Figure 4-1. Departments and agencies may also choose to use this zone for other department or agency-specific information, such as identifying a Federal emergency responder role, as depicted in Figure 4-2.	4.1.4.3/18	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-29	Zone 11—Agency Seal. If used, the seal selected by the issuing department, agency, or organization shall be printed in the area depicted. It shall be printed using the guidelines provided in Figure 4-2 to ensure information printed on the	4.1.4.3/19	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	seal is legible and clearly visible.								
2-30	Zone 12—Footer. The footer is the preferred location for the Emergency Response Official Identification label. If used, a department or agency may print "Federal Emergency Response Official" as depicted in Figure 4-2, preferably in red text. Departments and agencies may also print a secondary line in Zone 9 to further identify the Federal emergency respondent's official role. Some examples of official roles are "Law Enforcement, "Firefighter" and "Emergency Response Team (ERT)".	4.1.4.3/19	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-31	Zone 13—Issue Date. If used, the card issuance date shall be printed above the expiration date in YYYYMMMDD format as depicted in Figure 4-2.	4.1.4.3/19	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-32	Zone 15—Color-Coding for Employee Affiliation. Color-coding may be used for additional identification of employee affiliation. If color-coding is used, it shall be used as a background color for Zone 2 (name) as depicted in Figure 4-4. The following color scheme shall be used for the noted categories: + Blue—foreign nationals + Red—emergency responder officials + Green—contractors. These colors shall be reserved and shall not be employed for other purposes. Zone 15 may be a solid or patterned line at the department or agency's discretion.	4.1.4.3/19	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-33	Zone 16—Photo Border for Employee Affiliation. A border may be used with the photo to further identify employee	4.1.4.3/19	Optional Items on the Front of the	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	affiliation, as depicted in Figure 4-3. This border may be used in conjunction with Zone 15 to enable departments and agencies to develop various employee categories. The photo border shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the department or agency's discretion.		Card						
2-34	Zone 17—Agency Specific Data. In cases in which other defined optional elements are not used, Zone 17 may be used for other department or agency-specific information, as depicted in Figure 4-5.	4.1.4.3/19	Optional Items on the Front of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-35	Zone 3—Magnetic Stripe. If used, the magnetic stripe shall be high coercivity and placed in accordance with [ISO7811], as illustrated in Figure 4-7.	4.1.4.4/19	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-36	Zone 4—Return To. If used, the "return if lost" language shall be generally placed on the back of the card as depicted in Figure 4-7.	4.1.4.4/19	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-37	Zone 5—Physical Characteristics of Cardholder. If used, the cardholder physical characteristics (e.g., height, eye color, hair color) shall be printed in the general area illustrated in Figure 4-7.	4.1.4.4/19	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-38	Zone 6—Additional Language for Emergency Responder Officials. Departments and agencies may choose to provide additional information to identify emergency response officials or to better identify the cardholder's authorized access. If used, this additional text shall be in the general	4.1.4.4/19	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	area depicted and shall not interfere with other printed text or machine-readable components. An example of a printed statement is provided in Figure 4-7.								
2-39	Zone 7—Standard Section 499, Title 18 Language. If used, standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the card shall be printed in the general area depicted in Figure 4-7.	4.1.4.4/20	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-40	Zone 8—Linear 3 of 9 Bar Code. If used, a linear 3 of 9 bar code shall be generally placed as depicted in Figure 4-7. It shall be in accordance with Association for Automatic Identification and Mobility (AIM) standards. Beginning and end points of the bar code will be dependent on the embedded contactless module selected. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.	4.1.4.4/20	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-41	Zone 9—Agency-Specific Text. In cases in which other defined optional elements are not used, Zone 9 may be used for other department or agency-specific information, as depicted in Figure 4-8. For example, emergency responder officials may use this area to provide additional details.	4.1.4.4/20	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-42	In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by the Geneva Accord and to facilitate medical entitlements that are legislatively mandated.	4.1.4.4/20	Optional Items on the Back of the Card	PIV Card	Card Issuance and Management	Card	Component -Card	S	
2-43	To support a variety of authentication mechanisms, the PIV logical credentials shall contain multiple data elements for	4.1.5.1/29	Logical Credential Data Model	PIV Card	Front-End	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements collectively comprise the data model for PIV logical credentials, and include the following: + A PIN + A CHUID + PIV authentication data (one asymmetric key pair and corresponding certificate) + Two biometric fingerprints.								
2-44m	The PIV data model may be optionally extended to meet department or agency-specific requirements. If the data model is extended, this standard establishes requirements for the following four classes of logical credentials: + An asymmetric key pair and corresponding certificate for digital signatures + An asymmetric key pair and corresponding certificate for key management + Asymmetric or symmetric card authentication keys for supporting additional physical access applications + Symmetric key(s) associated with the card management system.	4.1.5.1/29	Logical Credential Data Model	Key Management	Front-End	Card	Component -Card	G	
2-45	PIV Cards shall implement PIN-based cardholder activation to allow privileged operations using PIV credentials held by the card.	4.1.6.1/30	Activation by Cardholder	PIN Input Device	Front-End	Card	Component -Keyboard -Biometric Reader	S	
2-46	For PIN-based cardholder activation, the cardholder shall supply a numeric PIN.	4.1.6.1/30	Activation by Cardholder	PIN Input Device	Front-End	Card	Component -Keyboard -Biometric Reader	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
							-Pin Reader		
2-47	The PIN shall be transmitted to the PIV Card and checked by the card. If the presented PIN is correct, the PIV Card is activated.	4.1.6.1/30	Activation by Cardholder	PIN Input Device	Front-End	Card	Component -Card -Keyboard -Biometric Reader -Pin Reader	S	
2-48	The PIV Card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen.	4.1.6.1/30	Activation by Cardholder	PIV Card	Front-End	Card	Component -Card	S	
2-49	Moreover, the PIN should not be easily-guessable or otherwise individually-identifiable in nature (e.g., part of a Social Security Number, phone number).	4.1.6.1/30	Activation by Cardholder	PIV Card	Front-End	Card	Component -Card	G	
2-50	The PIN authentication mechanism shall meet the identity-based authentication requirements of FIPS PUB 140-2 Level 2. [FIPS140-2]	4.1.6.1/30	Activation by Cardholder	PIV Card	Front-End	Card	Component -Card	S	
2-51m	PIV Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73].	4.1.6.2/30	Activation by Card Management System	PIV Card	Front-End	Card	Component -Card -Card Mgmt System -Card Writer	S	2-51m conflicts with 2-52
2-52	When cards are personalized, card management keys shall be set to be specific to each PIV Card. That is, each PIV Card shall contain a unique card management key.	4.1.6.2/30	Activation by Card Management System	Key Management	Front-End	Card	Component -Card -Card Writer	S	
2-53	Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal	4.1.6.2/30	Activation by Card Management System	Key Management	Front-End	Card	Component -Card -Card Writer	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	Identity Verification. [SP800-78]								
2-54	The PIV Card shall include the CHUID as defined in [SP800-73]. The CHUID includes an element, the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card.	4.2/30	Cardholder Unique Identifier (CHUID)	PIV Card	Front-End	Card	Component -Card	S	800-85 D.2
2-55	The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation.	4.2/30	Cardholder Unique Identifier (CHUID)	PIV Card	Front-End	Card	Component -Card	S	800-85 C1.1.2
2-56	The PIV FASC-N shall not be modified post-issuance.	4.2/30	Cardholder Unique Identifier (CHUID)	PIV Card	Front-End	Card	Component -Card -Card Mgmt System	S	
2-57	In addition to the mandatory FASC-N that identifies a PIV Card, the CHUID shall include an expiration date. In machine readable format, the expiration date data element shall specify when the card expires. The expiration date format and encoding rules are as specified in [SP800-73].	4.2.1/30	PIV CHUID Data Elements	PIV Card	Front-End	Card	Component -Card	S	800-85 C.1.2
2-58	This standard requires inclusion of the Asymmetric Signature field in the CHUID container. The Asymmetric Signature data element of the PIV CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as defined in RFC 3852 [RFC3852].	4.2.2/30	Asymmetric Signature Field in CHUID	PIV Card	Front-End	Card	Component -Card	S	800-85 D.2
2-59	The digital signature shall be computed over the entire contents of the CHUID, excluding the Asymmetric Signature field.	4.2.2/30	Asymmetric Signature Field in CHUID	PIV Card	Front-End	Card	Component -Card	S	800-85 D.2
2-60	The issuer asymmetric signature file is implemented as a SignedData Type, as specified in [RFC3852], and shall	4.2.2/30	Asymmetric Signature Field in	PIV Card	Card Issuance and Management	Card	Component -Card	S	800-85 D.2

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	include the following information: + The message shall include a version field specifying version v3 + The digestAlgorithms field shall be as specified in [SP800-78] + The encapContentInfo shall: – Specify an eContentType of id-PIV CHUIDSecurityObject – Omit the eContent field + The certificates field shall include only a single X.509 certificate which can be used to verify the signature in the SignerInfo field + The crls field shall be omitted + signerInfos shall be present and include only a single SignerInfo + The SignerInfo shall: – Use the issuerAndSerialNumber choice for SignerIdentifier – Specify a digestAlgorithm in accordance with [SP800-78] – Include, at a minimum, the following signed attributes: • A MessageDigest attribute containing the hash computed over the concatenated contents of the CHUID, excluding the asymmetric signature field • A pivSigner-DN attribute containing the subject name that appears in the PKI certificate for the entity that signed the CHUID – Include the digital signature.		CHUID						

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
2-61	The public key required to verify the digital signature shall be provided in the certificates field in an X.509 digital signature certificate issued under [COMMON], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3.	4.2.2/31	Asymmetric Signature Field in CHUID	Key Management	Front-End	Card PKI	Component -Card	S	800-85 D.8
2-63	The certificate shall also include an extendedKeyUsage extension asserting id-PIV-content-signing	4.2.2/31	Asymmetric Signature Field in CHUID	Key Management	Front-End	Card PKI	Component -Card	S	800-85 D.2
2-64	At a minimum, the PIV Card must store one asymmetric private key and a corresponding public key certificate, and perform cryptographic operations using the asymmetric private key. Cryptographic operations with this key are performed only through the contact interface *(GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR command).*	4.3/31	Cryptographic Specifications	Key Management	Front-End	Card PKI	Component -Card	S	800-85 C.3.2.2 D.8
2-65	The PIV Card shall implement the following cryptographic operations and support functions: + RSA or elliptic curve key pair generation + RSA or elliptic curve private key cryptographic operations + Importation and storage of X.509 certificates.	4.3/31	Cryptographic Specifications	Key Management	Front-End	Card PKI	Component -Card	G	
2-66m	The PIV Card may include additional asymmetric keys and PKI certificates.	4.3/32	Cryptographic Specifications	Key Management	Front-End	Card PKI	Component -Card	G	
2-67e	Where digital signature keys are supported, the PIV Card is not required to implement a secure hash algorithm.	4.3/32	Cryptographic Specifications	Key Management	Front-End	Card PKI	Component -Card -applications	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
2-68m	Message hashing may be performed off-card.	4.3/32	Cryptographic Specifications	PIV System	Front-End	Host PKI	Component -Host	G	
2-69	PIV Card must contain storage for the AES key and support AES operations through the contactless interface.	4.3/32	Cryptographic Specifications	PIV Card	Front-End	Card	Component -Card	S	conflicts with table?
2-70m	Cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a card authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize Advanced Encryption Standard (AES) based challenge/response for physical access, the PIV Card must contain storage for the AES key and support AES operations through the contactless interface. If the contactless interface utilizes asymmetric cryptography (e.g., elliptic curve cryptography [ECC]), the PIV Card may also require storage for a corresponding public key certificate.	4.3/32	Cryptographic Specifications	PIV Card	Front-End	Card	Component -Card	G	
2-71	All cryptographic operations using the PIV keys shall be performed on-card; the PIV Card need not implement any additional cryptographic functionality (e.g., hashing, signature verification) by additional cryptographic mechanisms implemented on-card. Algorithms and key sizes for each PIV key type are specified in [SP800-78].	4.3/32	Cryptographic Specifications	PIV Card	Front-End	Card	Component -Card	G	
2-72	The PIV authentication key shall be an asymmetric private key supporting card authentication for an interoperable	4.3/32	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	S	C 1.4 E.2

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	environment, and it is mandatory for each PIV Card.								
2-73m	The card authentication key may be either a symmetric (secret) key or an asymmetric private key for physical access, and it is optional.	4.3/32	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	G	
2-74	The digital signature key is an asymmetric private key supporting document signing, and it is optional.	4.3/32	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	G	
2-75	The key management key is an asymmetric private key supporting key establishment and transport, and it is optional. This can also be used as an encryption key.	4.3/32	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	S	
2-76	All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.	4.3/32	Cryptographic Specifications	PIV System	Front-End	Card	Component -Card	G	
2-77	In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage.	4.3/32	Cryptographic Specifications	PIV Card	Front-End	Card	Component -Card	G	
2-78	PIV Authentication Key. This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV authentication key. The PIV authentication key must be available only through the contact interface of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation)	4.3/32	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	S	800-85 C.1.2.1 (22) AS05.03
2-79	The PIV Card shall store a corresponding X.509 certificate to support validation of the public key *(for Authentication key).* The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The	4.3/32	Cryptographic Specifications	Key Management PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -PKI	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	expiration date of the certificate must be no later than the expiration date of the PIV Card.								
2-80	Card Authentication Key. The PIV Card shall not permit exportation of the card authentication key. Private/secret key operations may be performed using this key without explicit user action (e.g., the PIN need not be supplied). This standard does not specify key management protocols or infrastructure requirements.	4.3/33	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card -Physical Security System	S	
2-81	Digital Signature Key. The PIV digital signature key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact interface of the PIV Card. Private key operations may not be performed without explicit user action.	4.3/33	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card -Applications	S	
2-82	The PIV Card shall store a corresponding X.509 certificate to support validation of the digital signature key.	4.3/33	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card -Applications -PKI	S	
2-83	Key Management Key. This key may be generated on the PIV Card or imported to the card. If present, the key management key must only be accessible using the contact interface of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation). This key is sometimes called an encryption key or an encipherment key. The PIV Card shall import and store a	4.3/33	Cryptographic Specifications	Key Management PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	corresponding X.509 certificate to support validation of the key management key. Section 5.4 of this document specifies the certificate format and the key management infrastructure for PIV key management keys.								
2-84	Card Management Key. The card management key is imported onto the card by the issuer. If present, the card management key must only be accessible using the contact interface of the PIV Card.	4.3/33	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	S	
2-85m	The PIV Card may also import and store X.509 certificates for use in PKI path validation. These trust anchor certificates may be accessed through the contact interface using an activated PIV Card without explicit cardholder action.	4.3/33	Cryptographic Specifications	PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -PKI	S	
2-86m	If supported, initialization and update of trust anchor certificates shall require explicit cardholder action, in addition to activation of the card.	4.3/33	Cryptographic Specifications	Key Management PIV Card	Front-End	Card	Component -Card	S	
2-87	The biometric data used during the PIV Card life cycle activities shall consist of the following: + A full set of fingerprints used to perform law enforcement checks as part of the identity proofing and registration process + An electronic facial image used for printing facial image on the card as well as for performing visual authentication during card usage. A new facial image must be collected at the time of reissuance. The facial image is not required to be stored on the card. + Two electronic fingerprints to be stored on the card for	4.4/33	Biometric Data Specifications	PIV Card Biometric Reader Identity Proofing & Registration	Front-End	Card	Component -Card -Biometric Reader -Host	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	automated authentication during card usage. All three biometric data enumerated above are collected during the identity proofing and registration process. Implementation requirements for storage of biometric data on PIV Cards is dependent on use of specifications contained in NIST SP 800-76 [SP800-76].								
2-88	The two electronic fingerprints stored on the card shall be accessible only over the contact interface and after the presentation of a valid PIN.	4.4/34	Biometric Data Specifications	PIV Card Biometric Reader	Front-End	Card	Component -Card -Biometric Reader -Pin Reader -Host	S	
2-89	No contactless access is permitted for the biometric data specified to be stored on the PIV Card under this standard.	4.4/34	Biometric Data Specifications	PIV Card Biometric Reader	Front-End	Card	Component -Card -Biometric Reader -Host	S	?
2-90	The full set of fingerprints shall be collected from all PIV Card applicants who can provide them. The technical specifications for the collection and formatting of the ten fingerprints is contained in [SP800-76].	4.4.1/34	Biometric Data Collection, Storage, and Usage	Identity Proofing & Registration	Card Issuance & Management	Card	Component -Card -Biometric Reader -Host	S	
2-91	The fingerprints shall be used for one-to-many matching with the database of fingerprints maintained by the FBI.	4.4.1/34	Biometric Data Collection, Storage, and Usage	Identity Proofing & Registration	Card Issuance & Management	Card	Component -Issuance Scanner -Host System	G	
2-92	The fingerprints should be captured using FBI-certified scanners and transmitted using FBI standard transactions.	4.4.1/34	Biometric Data Collection, Storage, and Usage	Identity Proofing & Registration	Card Issuance & Management	Card Issuance	Component -Card -Issuance Scanner -Host System	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
2-93	A facial image shall be collected from all PIV applicants. The technical specifications for an electronic facial image are contained in [SP800-76].	4.4.1/34	Biometric Data Collection, Storage, and Usage	Identity Proofing & Registration	Card Issuance & Management	Card Issuance	Component -Card -Issuance Scanner -Host System	S	
2-94m	The electronic facial image may be used for the following purposes: + For generating the printed image on the card + For generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.1. This approach may be required in the following situations: – A good live sample of fingerprints cannot be collected from the PIV cardholder due to damage or injury to fingers – Fingerprint matching equipment failure – Authenticating PIV cardholders covered under Section 508.	4.4.1/34	Biometric Data Collection, Storage, and Usage	Identity Proofing & Registration	Card Issuance & Management	Card Issuance	Component -Card -Issuance Scanner -Host System	G	
2-95m	Two electronic fingerprints shall be collected from all PIV applicants, who can provide them, for storing on the card. Alternatively, these two electronic fingerprints can also be extracted from the ten fingerprints collected earlier for law enforcement checks. The technical specifications for the two electronic fingerprints are contained in [SP800-76]. The right and left index fingers shall normally be designated as the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary and secondary designations shall be taken from the following	4.4.1/34	Biometric Data Collection, Storage, and Usage	Identity Proofing & Registration	Card Issuance & Management	Card Issuance	Component -Card -Issuance Scanner -Host System	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	fingers, in decreasing order of priority: 1. Right thumb 2. Left thumb 3. Right middle finger 4. Left middle finger 5. Right ring finger 6. Left ring finger 7. Right little finger 8. Left little finger								
2-96	Even though two fingerprints are available on the card, a department or agency has the option to use one or both of them for the purpose of PIV cardholder authentication. If only one fingerprint is used for authentication, then the primary finger shall be used first. In cases where there is difficulty in collecting even a single fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography as described in Section 6.2.4.	4.4.1/34	Biometric Data Collection, Storage, and Usage	PIV Card	Card Issuance & Management	Card Issuance	Component -Card -Issuance Scanner -Host System	G	
2-97	The format for CBEFF_HEADER and the STD_BIOMETRIC_RECORD is specified in [SP800-76].	4.4.1/35	Biometric Data Collection, Storage, and Usage	PIV Card	Front-End	Card Issuance	Component -Card	S	
2-98	The digital signature shall be computed over the entire CBEFF structure except the CBEFF_SIGNATURE_BLOCK itself (which means that it includes the CBEFF_HEADER and STD_BIOMETRIC_RECORD).	4.4.1/35	Biometric Data Collection, Storage, and Usage	PIV Card	Front-End	Card Issuance	Component -Card	S	
2-99	The CMS encoding of the CBEFF_SIGNATURE_BLOCK is as a SignedData type, and shall include the following information: + The message shall include a version field specifying version v3 + The digestAlgorithms field shall be as specified in [SP800-78]	4.4.2/35	Biometric Data Representation and Protection	PIV Card	Front-End	Card Issuance	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	+ The encapcontentInfo shall – Specify an eContentType of id-PIV-biometricObject – Omit the eContent field + If the signature on the biometric was generated with the same key as the signature on the CHUID, the certificates field shall be omitted + If the signature on the biometric was generated with a different key as the signature on the CHUID, the certificates field shall include only a single certificate which can be used to verify the signature in the SignerInfo field + The crls field shall be omitted + signerInfos shall be present and include only a single SignerInfo + The SignerInfo shall – Use the issuerAndSerialNumber choice for SignerIdentifier – Specify a digestAlgorithm in accordance with [SP800-78] Include at a minimum the following signed attributes: • A MessageDigest attribute containing the hash of the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD • A pivFASC-N attribute containing the FASC-N of the PIV Card (to link the biometric data and PIV Card)								

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	• A pivSigner-DN attribute containing the subject name that appears in the PKI certificate for the entity that signed the biometric data – Include the digital signature.								
2-100	Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface.	4.5.1/37	Contact Reader Specifications	Card Reader/Writer	Front-End	Card Issuance	Component -Card -Card Reader -Host System	S	
2-101	These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface in general desktop computing environment.	4.5.1/37	Contact Reader Specifications	Card Reader/Writer	Front-End	Reader	Component -Card - Card Reader -Host System	S	
2-102	In physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this standard.	4.5.1/37	Contact Reader Specifications	Card Reader/Writer	Front-End	Reader	Component -Card Reader -Host System -Desktop	S	
2-103	Contactless card readers shall conform to the [ISO 14443] standard for the card-to-reader interface.	4.5.2/37	Contactless Reader Specifications	Card Reader/Writer	Front-End	Card	Component -Card Reader -Host System	G	
2-104	In cases where these readers are connected to general purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-host system interface.	4.5.2/37	Contactless Reader Specifications	Card Reader/Writer	Front-End	Card	Component -Card Reader -Desktop	S	
2-105	PIN input devices shall be used for implementing PIN-based PIV Card activation.	4.5.3/37	PIN Input Device Specifications	PIN Input Device	Front-End	PIN Reader	Component - PIN Reader -Host System	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
2-106	When the PIV Card is used with a PIN for physical access, the PIN input device shall be integrated with the reader.	4.5.3/37	PIN Input Device Specifications	PIN Input Device	Front-End	PIN Reader	Component - PIN Reader - Biometric Reader -Host System	S	
2-107m	When the PIV Card is used with a PIN for logical access (e.g., to authenticate to a Web site or other server), the PIN input device may be integrated with the reader or entered using the computer's keyboard.	4.5.3/37	PIN Input Device Specifications	PIN Input Device	Front-End	PIN Reader	Component - PIN Reader -Desktop	S	
2-108	If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation.	4.5.3/37	PIN Input Device Specifications	PIN Input Device	Front-End	PIN Reader	Component - PIN Reader -Desktop	S	
2-109	Each agency's PIV implementation(s) shall support interoperability by issuing and managing interoperable PIV Cards and their associated logical credentials specified in Section 4.	5.1/38	Control Objectives and Interoperability Requirements	PIV System	Card Issuance and Management Subsystem	PIV System	Component - PIV System	G	
2-110	All PIV-II identity proofing and registration systems must satisfy the PIV-I objectives and requirements stated in Section 2.2 in order to be approved.	5.2/39	PIV Identity Proofing and Registration Requirements	PIV System	Card Issuance and Management Subsystem	Cards	Component - PIV System	G	
2-111	An additional requirement for PIV-II is that the biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during the identity proofing and registration process.	5.2/39	PIV Identity Proofing and Registration Requirements	Identity Proofing & Registration	Card Issuance and Management Subsystem	Cards	Component - PIV Card -Scanner	S	
2-112	When issuing PIV Cards, Federal agencies and departments must use an approved identity proofing and registration	5.2/39	PIV Identity Proofing and	Identity Proofing & Registration	Card Issuance and Management	Cards	Component - PIV Card	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	process. Two approved PIV identity proofing and registration processes are provided in Appendix A. Other identity proofing and registration process may be used if accredited by the department or agency as satisfying the requisite PIV objectives and requirements and approved in writing by the head of the Federal department or agency.		Registration Requirements		Subsystem		-Scanner		
2-113	An employee or contractor may be issued PIV Card and logical credentials while a National Agency Check with Written Inquiries (NACI) or other OPM or National Security community investigation required for Federal employment is pending. In such cases, the process must verify successful completion and adjudication of the investigation within six months of PIV card issuance, or the PIV card and the PIV authentication certificate for the card shall be revoked.	5.3.1/39	PIV Card Issuance	Identity Proofing & Registration	Card Issuance and Management Subsystem	Cards	Component - PIV Card -Scanner	G	
2-114	An additional requirement is that the issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record. On successful match, the PIV Card shall be released to the applicant.	5.3.1/39	PIV Card Issuance	Identity Proofing & Registration	Card Issuance and Management Subsystem	Cards	Component - PIV Card -Scanner	S	
2-115	The heads of Federal departments and agencies may approve other identity proofing, registration, issuance process sets that are accredited as satisfying the requisite PIV-I objectives and requirements.	5.3.1/39	PIV Card Issuance	Identity Proofing & Registration	Card Issuance and Management Subsystem	Cards	Component - PIV System	G	
2-116	The card issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials to current employees, the	5.3.2/39	PIV Card Maintenance	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Process	Component -Card Issuer -NACI check	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	NACI checks shall be followed in accordance with the OPM guidance.								
2-117	The data and credentials held by the PIV Card may need to be invalidated prior to the expiration date of the card. The cardholder may retire, change jobs, or the employment is terminated, thus requiring invalidation of a previously active card. The card may be damaged, lost, or stolen, thus requiring a replacement. The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card management.	5.3.2/39	PIV Card Maintenance	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Process	Component - PIV System	G	
2-118	The PIV Card shall be valid for no more than five years.	5.3.2.1/39	PIV Card Renewal	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Card	Component - PIV Card	S	
2-119	A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card.	5.3.2.1/39	PIV Card Renewal	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Process	Component - PIV Card	S	
2-120	The card issuer will verify the cardholder's identity against the biometric information stored on the expiring card.	5.3.2.1/39	PIV Card Renewal	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Process	Component - PIV Card	S	
2-121	The expired PIV Card must be collected and destroyed.	5.3.2.1/39	PIV Card Renewal	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Process	Component - PIV Card	S	
2-122m	The same biometric data may be reused with the new PIV	5.3.2.1/39	PIV Card Renewal	Card Issuance &	Card Issuance	Process	Component	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	Card while the digital signature must be recomputed with the new FASC-N.			Maintenance	and Management Subsystem		- PIV Card		
2-123	The expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card. Hence, a new PIV authentication key and certificate shall be generated.	5.3.2.1/39	PIV Card Renewal	Card Issuance & Maintenance PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PIV Card -PKI	S	
2-124m	If the PIV Card supports the optional key management key, it may be imported to the new PIV Card.	5.3.2.1/39	PIV Card Renewal	Card Issuance & Maintenance PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PIV Card -PKI	S	
2-125	In case of reissuance, the entire registration and issuance process, including fingerprint and facial image capture, shall be conducted.	5.3.2.2/40	PIV Card Reissuance	Card Issuance & Maintenance PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PIV Card -PKI -Issuance Scanner	G	
2-126	The card issuer shall verify that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.	5.3.2.2/40	PIV Card Reissuance	Card Issuance & Maintenance	Card Issuance and Management Subsystem	Process	Component - PIV Card	G	
2-127	The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder.	5.3.2.2/40	PIV Card Reissuance	Card Issuance & Maintenance PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PIV Card -PKI	S	
2-128	It is recommended that the old PIV Card, if available, is collected and destroyed. If the card cannot be collected,	5.3.2.2/40	PIV Card Reissuance	Card Issuance & Maintenance	Card Issuance and Management	Process	Component - PIV Card	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	normal operational procedures shall complete within 18 hours of notification. In some cases, 18 hours is an unacceptable delay. In that case, emergency procedures must be executed to disseminate this information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.			PKI Directory & Certificate Status Responder	Subsystem		-PKI		
2-129	A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of an employee status or attribute change or if one or more logical credentials have been compromised. When these events are reported, normal operational procedures must be in place to ensure the following: + The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status. + The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers. + Online Certificate Status Protocol (OCSP) responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be	5.3.2.2/40	PIV Card Reissuance	Card Issuance & Maintenance PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PIV Card -PKI	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).								
2-130	Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card.	5.3.2.3/40	PIV Card PIN Reset	Biometric Reader PIN Input Device Card Issuance & Maintenance	Card Issuance and Management Subsystem	Card	Component -Card -Biometric Reader -Pin Reader -Host System	S	
2-131m	The PIN on a PIV Card may need to be reset if the contents of the card are locked resulting from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency. PIN resets may be performed by the card issuer.	5.3.2.3/40	PIV Card PIN Reset	PIN Input Device Card Issuance & Maintenance	Card Issuance and Management Subsystem	Card	Component -Card -Pin Reader -Host System	S	
2-132	The termination process is used to permanently destroy or invalidate the use of the card, including the data and the keys on it, such that it cannot be used again. The PIV Card shall be terminated under the following circumstances: + An employee separates (voluntarily or involuntarily) from Federal service + An employee separates (voluntarily or involuntarily) from a Federal contractor + A contractor changes positions and no longer needs access to Federal buildings or systems + A cardholder is determined to hold a fraudulent identity + A cardholder passes away.	5.3.2.4/41	PIV Card Termination	PIV System	Card Issuance and Management Subsystem	Card	Component -Card -PIV System	G	
2-133	Similar to the situation in which the card or a credential is	5.3.2.4/41	PIV Card	PIV System	Card Issuance	Card	Component	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	compromised, normal termination procedures must be in place as to ensure the following: + The PIV Card is collected and destroyed. + The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status. + The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers. + OCSP responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records). + The IIF that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.		Termination	PKI Directory & Certificate Status Responder	and Management Subsystem		-Card -PIV System -PKI		
2-134	The CA that issues certificates to support PIV Card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI.	5.4.1/41	Architecture	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component -PKI	S	
2-135	Self-signed, self-issued, and CA certificates issued by these CAs shall conform to Worksheet 1: Self-Signed Certificate Profile, Worksheet 2: Self-Issued CA Certificate Profile, and Worksheet 3: Cross Certificate Profile, respectively, in	5.4.1/41	Architecture	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component -Card -PKI	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	X.509 Certificate and CRL Profile for the Common Policy [PROF].								
2-136	All certificates issued to support PIV Card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy as defined in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON].	5.4.2/41	PKI Certificate	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component -Card -PKI	S	
2-137	CAs and registration authorities may be operated by departments and agencies, or outsourced to PKI service providers.	5.4.2/41	PKI Certificate	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component -Card -PKI	S	
2-138	[COMMON] requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (i.e., the PIV Card).	5.4.2/41	PKI Certificate	PIV Card	Card Issuance and Management Subsystem	PKI	Component -Card	S	
2-139	In addition, this standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.	5.4.2/42	PKI Certificate	PIV Card PKI Directory & Certificate Status Responder	Front-End Card Issuance and Management Subsystem	Card	Component -Card - Pin Reader -Desktop	S	
2-140	[COMMON] specifies the use of RSA along with the key sizes and hash functions.	5.4.2/42	PKI Certificate	PIV Card PKI Directory & Certificate Status Responder	Front-End Card Issuance and Management Subsystem	Card	Component -Card - Pin Reader -Desktop	S	
2-141	This standard allows additional cryptographic algorithms and key sizes as specified in the [SP 800-78]. Future enhancements to [COMMON] are expected to permit use of additional algorithms. For conformance to this standard, PIV Card management systems are limited to algorithms and key sizes recognized by this standard and the current version of	5.4.2/42	PKI Certificate	PIV Card PKI Directory & Certificate Status Responder	Front-End Card Issuance and Management Subsystem	Card	Component -Card - Pin Reader -Desktop -PKI	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	[COMMON].								
2-142	The required contents of X.509 certificates associated with PIV private keys are based on [PROF]. The relationship is described below: + Authority Information Access (AIA) extensions shall include pointers to the appropriate OCSP status responders, using the id-ad-ocsp access method as specified in Section 8 of [PROF], in addition to the Lightweight Directory Access Protocol (LDAP) Uniform Resource Identifiers (URI) required by [PROF]. + If private key computations can be performed with the PIV authentication key without user intervention (beyond that required for cryptomodule activation), the corresponding certificate must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension. + Certificates containing the public key associated with an asymmetric Card Authentication Key must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension and must assert id-PIV-cardAuth in the extended key usage extension. + Certificates containing the public key associated with a digital signature private key shall conform to Worksheet 5: End Entity Signature Certificate Profile in [PROF]. + Certificates containing the public key associated with a PIV authentication private key shall conform to Worksheet 5: End Entity Signature Certificate Profile in [PROF], but shall not assert the nonRepudiation bit in the keyUsage	5.4.2/42	PKI Certificate	PIV Card PKI Directory & Certificate Status Responder	Front-End Card Issuance and Management Subsystem	Card	Component -Card - PKI	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	extension and must include the PIV Card's FASC-N in the subject alternative name field. + Certificates containing the public key associated with a key management private key shall conform to Worksheet 6: Key Management Certificate Profile in [PROF]. + Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP800-78].								
2-143	CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to Worksheet 4: CRL Profile in [PROF].	5.4.3/43	X.509 CRL Contents	PIV Card PKI Directory & Certificate Status Responder	Front-End Card Issuance and Management Subsystem	Card	Component -Card - PKI	S	
2-144	Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)	5.4.4/43	Migration from Legacy PKIs	PIV Card PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component - PKI	S	
2-145	The expiration date of the authentication certificate shall not be after the expiration date of the PIV Card. If the card is revoked, the authentication certificate shall be revoked. However, an authentication certificate (and its associated key pair) may be revoked without revoking the PIV Card and may then be replaced. The presence of a valid,	5.4.5/43	PKI Repository and OCSP Responder(s) PIV Card	PIV Card PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Card	Component - PKI -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	unexpired, and unrevoked PIV authentication certificate on a card is proof that the card was issued and is not revoked.								
2-146	CAs that issue PIV authentication certificates shall maintain a LDAP directory server that holds the CRLs for the certificates it issues, as well as any CA certificates needed to build a path to the Federal Bridge CA.	5.4.5/43	PKI Repository and OCSP Responder(s)	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component - PKI (LDAP Server)	S	
2-147	Certificates shall contain the crlDistributionPoints or authorityInfoAccess extensions needed to locate CRLs and the authoritative OCSP responder.	5.4.5/43	PKI Repository and OCSP Responder(s)	PIV Card PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component - PKI -Card	S	
2-148	In addition, every CA that issues PIV authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues.	5.4.5/43	PKI Repository and OCSP Responder(s)	PIV Card PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component - PKI -Card	S	
2-149	This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP). Specific requirements are found in Table II—Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements of the Shared Service Provider Repository Service Requirements [SSP REP].	5.4.5.1/43	Certificate and CRL Distribution	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component - PKI	G	
2-150	PIV Authentication certificates contain the FASC-N in the subject alternative name extension; hence, these certificates shall not be distributed publicly via LDAP or HTTP.	5.4.5.1/43	Certificate and CRL Distribution	PIV Card PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	PKI	Component - PKI -Card	S	
2-151	When user certificates are distributed, the requirements in Table I—End-Entity Certificate Repository Service Requirements of [SSP REP] shall be satisfied.	5.4.5.1/43	Certificate and CRL Distribution	PIV Card PKI Directory & Certificate Status	Card Issuance and Management Subsystem	PKI	Component - PKI -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
				Responder					
2-152	OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status mechanism.	5.4.5.2/44	OCSP Status Responders	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PKI	S	
2-153	The OCSP status responders must be updated at least as frequently as CRLs are issued.	5.4.5.2/44	OCSP Status Responders	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PKI	S	
2-154	The definitive OCSP responder for each certificate shall be specified in the AIA extension as described in [PROF].	5.4.5.2/44	OCSP Status Responders	PKI Directory & Certificate Status Responder	Card Issuance and Management Subsystem	Process	Component - PKI -Card	S	
2-155	The PIV Privacy Requirements stated in Section 2.4 apply equally to PIV-II implementations.	5.5/44	PIV Privacy Requirements	PIV System	Card Issuance and Management Subsystem	Process	Component -PIV System	G	
2-156	Visual authentication of a PIV cardholder shall be used only to support access control to physical facilities and resources.	6.2.1/46	Authentication Using PIV Visual Credentials (VIS)	PIV Card Biometric Reader	Front-End	Process	Component -Card -Biometric Reader -Pin Reader -Host System	S	
2-157	The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication, as follows: + Photograph + Name + Employee affiliation employment identifier + Expiration date + Agency card serial number (back of card) + Issuer identification (back of card).	6.2.1/46	Authentication Using PIV Visual Credentials (VIS)	PIV Card	Front-End	Process	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
2-158	When a cardholder attempts to pass through an access control point for a Federally controlled facility, a human guard shall perform visual identity verification of the cardholder, and determine whether the identified individual should be allowed through the control point. The series of steps that shall be applied in the visual authentication process are as follows: 1. The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way. 2. The guard compares the cardholder's facial features with the picture on the card to ensure that they match. 3. The guard checks the expiration date on the card to ensure that the card has not expired. 4. The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional) 5. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional) 6. One or more of the other data elements on the card (e.g., name, employee affiliation employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.	6.2.1/46	Authentication Using PIV Visual Credentials (VIS)	PIV Card	Front-End	Process	Component -Card	S	
2-159	The CHUID shall be used for PIV cardholder authentication using the following sequence: 1. The CHUID is read electronically from the PIV Card.	6.2.2/48	Authentication Using the PIV CHUID	PIV Card PKI Directory & Certificate Status	Front-End	Card	Component -Card -Host System	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered. (Optional) 3. The expiration date is checked to ensure that the card has not expired. 4. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Numbering System [DUNS]) are used as input to the authorization check to determine whether the cardholder should be granted access.			Responder			-PKI		
2-160	The following sequence shall be followed for unattended authentication of the PIV biometric: 1. The CHUID is read from the card. 2. The Expiration Date in the CHUID is checked to ensure the card has not expired. 3. The cardholder is prompted to submit a PIN, activating the PIV Card. 4. The PIV biometric is read from the card. 5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional) 6. The cardholder is prompted to submit a live biometric sample. 7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card. 8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital	6.2.3.1/48	Unattended Authentication Using PIV Biometric (BIO)	PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -Biometric Reader -PIN Reader -Host System -PKI	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	signature on the biometric. 9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.								
2-161	The following sequence shall be followed for attended authentication of the PIV biometric: 1. The CHUID is read from the card. 2. The Expiration Date in the CHUID is checked to ensure that the card has not expired. 3. The cardholder is prompted to submit a PIN. The PIN entry is done in the view of an attendant. 4. The submitted PIN is used to activate the card. The PIV biometric is read from the card. 5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional) 6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in the view of an attendant. 7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card. 8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric. 9. One or more of the CHUID data elements (e.g., FASC-N,	6.2.3.1/48	Attended Authentication Using PIV Biometric (BIO)	PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -Biometric Reader -PIN Reader -Host System -PKI	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access. This authentication mechanism is similar to the unattended biometric credential check; the only difference is that an attendant (e.g. security guard) supervises the use of the PIV Card and the submission of the PIN and the biometric by the cardholder.								
2-162	The PIV Card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4. The following steps shall be used to perform authentication using the PIV asymmetric authentication key: 1. The cardholder is prompted to submit a PIN. 2. The submitted PIN is used to activate the card. 3. The reader issues a challenge string to the card and requests an asymmetric operation in response. 4. The card responds to the previously issued challenge by signing it using the PIV authentication private key and attaching the associated certificate. 5. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity. 6. The response is validated as the expected response to the issued challenge.	6.2.3.1/49	Attended Authentication Using PIV Biometric (BIO)	PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -Biometric Reader -PIN Reader -Host System -PKI	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	7. The Subject Distinguished Name (DN) and FASC-N from the authentication certificate are extracted and passed as input to the authorization function.								
2-163m	The PIV Card can be used to authenticate the cardholder in a physical access control environment.	6.3.1/50	Physical Access	PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -Biometric Reader -PIN Reader -Host System -PKI	G	
2-164	It is implicit that an authentication mechanism *(Physical access)* that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.	6.3.1/50	Physical Access	PIV System	Front-End	PIV System	Component - PIV System	G	
2-165m	Each authentication mechanism described in the table can be further strengthened through the use of a back-end certificate status verification infrastructure, if the access control point has connectivity to the department or agency's network infrastructure.	6.3.1/50	Physical Access	PIV System	Front-End	PIV System	Component - PIV System -PKI	G	
2-166	The PIV Card may be used to authenticate the cardholder in support of decisions concerning access to logical information resources.	6.3.2/51	Logical Access	PIV Card PKI Directory & Certificate Status Responder	Front-End	Card	Component -Card -Biometric Reader -PIN Reader -Host System -PKI	G	
2-167	It is implicit that an authentication mechanism *(Logical access)* that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance	6.3.2/51	Logical Access	PIV System	Front-End	PIV System	Component - PIV System	G	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	level.								
2-168	Funding permitting, NIST will establish detailed criteria that PIV Card issues must meet for accreditation. Additionally, NIST will (again, funding permitting) establish a government-wide program to accredit official issuers of PIV Cards against these accreditation criteria. Until such time as these are completed, agencies must self-certify their own issuers of PIV Cards.	B.1/64	Accreditation of PIV Service Providers	PIV System	Front-End	PIV System	Component - PIV System	G	
2-169	In order to accomplish the accreditation of PIV service providers as described above, and to be compliant with the provisions of OMB Circular A-130, App. III, the IT system(s) used by PIV service providers must also be certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.	B.2/64	C&A of PIV service Providers	PIV System	Front-End	PIV System	Component - PIV System	G	
3-1	The contact interface of the PIV Card shall not require a Programming Voltage to operate correctly.	Interop. Reqs. 2.1.1.1	Card / Reader Interoperability Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	
3-2	The contact interface of the PIV Card shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002	Interop. Reqs. 2.1.1.2	Card / Reader Interoperability Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	
3-3	At a minimum, the contact interface of the PIV Card shall support either the T=0 or T=1 transmission protocol as defined in ISO/IEC 7816-3:1997. The card may support	Interop. Reqs. 2.1.1.3	Card / Reader Interoperability Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	both protocols								
3-4	PIV Cards shall not require the use of any RFU bits in the Global or Specific Interface Bytes to operate correctly.	Interop. Reqs. 2.1.1.4	Card / Reader Interoperability Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	
3-5	The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001	Interop. Reqs. 2.2.1.1	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-6	The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001	Interop. Reqs. 2.2.1.2	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-7	The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001	Interop. Reqs. 2.2.1.3	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-8	PIV Readers shall not generate a Programming Voltage.	Interop. Reqs. 2.2.2.1	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-9	PIV readers shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.	Interop. Reqs. 2.2.2.2	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
3-10	The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997	Interop. Reqs. 2.2.2.3	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-11	PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997	Interop. Reqs. 2.2.2.4	Card / Reader Interoperability Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-12	The reader-to-host interface for physical access control readers shall conform with one of the following standards: • Ethernet as defined in IEEE 802.3-2005, Standard for Information Technology-Telecommunications and Information Exchange Between Systems • RS-232 as defined in TIA-232, Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange • RS-485 as defined in TIA-485, Electrical Characteristics of Generators and Receivers For Use in Balanced Digital Multipoint Systems • Wiegand™ as defined in sections 3 and 4 of the SIA Access Control Standard Protocol for the 26-BIT Wiegand™ Reader Interface	Interop. Reqs. 2.2.3.1 through 2.2.3.4	Card / Reader Interoperability Requirements	PIV Reader	Physical Access Control	Reader	Component -Card -Reader	S	
3-13	Physical access control readers shall read the Agency Code, System Code and Credential Code elements of the FASC-N	Interop. Reqs.	Card / Reader Interoperability	PIV Reader	Physical Access Control	Reader	Component -Card	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
	along with the Expiration Date (YYYYMMDD) from the CHUID as defined by appendix A of NIST Special Publication 800-73. The reader shall output these four elements as concatenated individual binary numbers Parity bits shall be added to the beginning and end of the string providing a total length of 75 bits. The first bit transmitted is the first parity bit, P1, it is even parity calculated over the first 37 code bits. The last bit transmitted is the second parity bit, P2, it is odd parity calculated over the last 36 code bits.	2.2.3.5	Requirements				-Reader		
3-14	Retrieval time for 4 KB of data through the contactless interface of the card shall not exceed 3.0 seconds.	Interop. Reqs. 3.1.1.1	Electronic Authentication Performance Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	
3-15	Retrieval time for 22 KB of data through the contact interface of the card shall not exceed 2.0 seconds	Interop. Reqs. 3.1.2.1	Electronic Authentication Performance Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	
3-16	The reader buffer size shall be no less than 256 bytes	Interop. Reqs. 3.2.1	Electronic Authentication Performance Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-17	The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64 (~212 kbits/s), fc/32 (~424 kbits/s) and fc/16 (~847 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005	Interop. Reqs. 3.2.2.1	Electronic Authentication Performance Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested

Req#	Requirement	FIPS201 Ref. sect/pg	FIPS 201 Section Title	Applicable Component /System Function	PIV Subsystem	Target System (may be combine w impacts col)	Requirement Impacts: Process /Component -Type	Requirement Type* General / Specific/	BPA Approval Process #
3-18	Retrieval time for 4 KB of data through the contactless interface of the reader shall not exceed 3.0 seconds.	Interop. Reqs. 3.2.2.2	Electronic Authentication Performance Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-19	The PIV reader contact interface shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997	Interop. Reqs. 3.2.3.1	Electronic Authentication Performance Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-20	Retrieval time for 22 KB of data through the contact interface of the reader shall not exceed 2.0 seconds	Interop. Reqs. 3.2.3.2	Electronic Authentication Performance Requirements	PIV Reader	Card Issuance and Management	Reader	Component -Card -Reader	S	
3-21	Buffers shall not be readable through the contactless interface when the card is stored in an electromagnetically opaque sleeve at any distance	Interop. Reqs. 4.1.1.1	Security Related Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	
3-22	Buffers shall not be readable through the contactless interface more than 10 cm from the reader	Interop. Reqs. 4.1.1.2	Security Related Requirements	PIV Card	Card Issuance and Management	Card	Component -Card -Reader	S	

- General- applies to more than one subsystem, multiple test scenarios, implied by Specific requirement. Specific- applies to 1 subsystem .
- e- exclusive requirement- generally exclusive requirements are untested